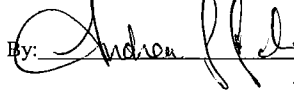


I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to:  
Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450  
On 11/3/07

PATENT  
Dckt. No.: 16222U-016100US  
Client Ref.: P-0088

TOWNSEND and TOWNSEND and CREW LLP

By:  Andrea S. Beck

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re application of:

DAVIS, STEVE

Application No.: 10/705,212

Filed: November 6, 2003

For: CENTRALIZED ELECTRONIC  
COMMERCE CARD TRANSACTIONS

Customer No.: 20350

Confirmation No. 2931

Examiner: Jalatee Worjloh

Technology Center/Art Unit: 3621


**DECLARATION UNDER  
37 C.F.R. § 1.131**

Sir:

I, Jonathan Hollander, declare as follows:

1. I am the attorney that prepared the above-referenced patent application.
2. I understand that claims 1-31 of this patent application are primarily rejected over U.S. Patent Application No. 2005/0021781 to Sunder et al. as a primary reference.
3. The acts relied on in this Declaration and described in the Exhibits took place in a WTO country after January 1, 1996.
4. The inventions of at least the pending claims were conceived of before June 5, 2003, which is the earliest noted priority date for Sunder et al.

5. Evidence of conception is shown by Exhibit A, which is a true copy of a technical specification entitled "3-D Secure Business Requirements and Technical Approach - VisaGold Version 1.0."
6. Exhibit A was provided to me by Steve Davis, the inventor of this application, on or before May 30, 2003.
7. The text and figures of Exhibit A are substantially similar to the text and figures of this patent application.
8. Exhibit A was prepared by the inventor on or before May 12, 2003. This is indicated by the date noted on the cover page of Exhibit A. Exhibit A thereby evidences a date of conception of the invention of claims 1-31 prior to the earliest priority date of Sunder et al.
9. As shown by Exhibits A, I believe that embodiments of the pending claims were conceived of before June 5, 2003, the earliest claimed priority date for Sunder et al., and that a patent application was diligently pursued thereafter.
10. I hereby declare that all statements made of my own knowledge are true and that all statements made on information and belief are believed to be true. I understand that willful false statements and the like are punishable by fine or imprisonment, or both (18 U.S.C. §1001) and may jeopardize the validity of the application or any patent issuing thereon.

  
Jonathan Hollander  
Reg. No. 48,717

1/3/2007  
Date

## **EXHIBIT A**



# **3-D Secure™**

## **Business Requirements and Technical Approach**

VisaGold

Version 1.0  
May 12, 2003  
S. Davis

*© 2003 Visa U.S.A. Inc. This information is Confidential and Proprietary, is distributed only by Visa U.S.A. for the use exclusively in operating this Visa-sponsored program, and shall not be duplicated, published, or disclosed, in whole or in part, without the written permission of Visa U.S.A.*

---

## Table of Contents

<b>1</b>	<b>INTRODUCTION .....</b>	<b>1</b>
<b>2</b>	<b>VISAGOLD GENERAL BUSINESS REQUIREMENTS .....</b>	<b>1</b>
2.1	PRIMARY BUSINESS OBJECTIVE PROVIDE VISIBILITY TO 3-D SECURE PROCESSING .....	1
2.2	PROVIDE A RESPONSE ON BEHALF OF AN ACS .....	2
2.3	PROVIDE A WAY TO MANAGE INTEROPERABILITY BETWEEN MPI'S AND ACS'S .....	2
2.4	AUTHENTICATION INTEGRITY, DATA QUALITY, AND SYSTEMATIC SOLUTION .....	2
<b>3</b>	<b>VISAGOLD APPROACH .....</b>	<b>2</b>
3.1	VISAGOLD BUSINESS REQUIREMENTS .....	2
3.2	VISAGOLD SERVICE AND TECHNICAL REQUIREMENTS .....	3
3.3	VISAGOLD PROCESS FLOW .....	5
3.4	VISAGOLD REPORTING REQUIREMENTS .....	9
3.5	OPTIONAL VERES MESSAGE EXTENSION .....	10
<b>4</b>	<b>RELATED DOCUMENTS .....</b>	<b>11</b>

# 1 Introduction

The 3-D Secure architecture uses a distributed computing model to communication messages between Verified by Visa enabled merchants and Access Control Servers (ACS). In this approach, no central point exists to collect information, monitor system performance, and report on the interaction between each of the transaction participants. In order to manage this service Visa must ask each end point – Issuers and merchants – to collect and provide statistics to Visa personnel in order to determine how the service is performing. The data available at each end point differs in the manner in which it is collected and quality and quantity of data available for collection. This approach to managing and monitoring the operational performance of the service has proven to be administratively cumbersome and time consuming, requiring a lot of support from each end point and Visa.

This document describes the general business requirements and technical approach to extend the existing 3-D Secure architecture to provide a systematic way to collect information, monitor system performance of each end point, and manage the interactions between these end points. This approach is referred to as *VisaGold*.

## 2 VisaGold General Business Requirements

There are a number of general business requirements that VisaGold must support. These are outlined below. More specific business requirements are described in subsequent sections.

### 2.1 *Primary Business Objective Provide Visibility to 3-D Secure Processing*

The primary business objective of VisaGold is to increase the reliability and monitoring of the Verified by Visa service by allowing Visa to participate in all of the 3-D Secure transaction flows. This means VisaGold will log all activity between each participant in a Verified by Visa transaction and provide a way to correlate each message cycle – VEReq/VERes, PAREq/PARes, and PATransReq/PATransRes – in to one complete view of a 3-D Secure authentication. Collection of this information will be used to measure, monitor, and report on the performance of Verified by Visa service end point.

## *2.2 Provide a Response on behalf of an ACS*

The VisaGold platform is between the DS and the ACS during VReq/VERes processing, between the cardholder and the ACS during PReq/PRes processing, and between the ACS and AHS during PTransReq/PTransRes processing. If an ACS becomes unavailable while processing an authentication request, or otherwise does not respond in a timely fashion, VisaGold can generate a response on behalf of the ACS. The implementation of VisaGold provides a high assurance that all Verified by Visa transactions will complete successfully.

## *2.3 Provide a way to Manage Interoperability between MPI's and ACS's*

The implementation of VisaGold will provide a way to manage the quality of data received from participating merchants by providing a single platform through which all transactions are processed. In the same manner, the implementation of VisaGold will also provide a way to manage the quality of data returned by participating Issuer ACS's.

## *2.4 Authentication Integrity, Data Quality, and Systematic Solution*

The Internet has proven to be a high growth market segment and is expected to represent significant sales volume over the years. The implementation of VisaGold provides a comprehensive way to record all Verified by Visa activity in a single place. This single source of information can be used to measure, manage, and monitor the operating characteristics for the entire Verified by Visa service. As such, there is a need to incorporate transaction integrity and data quality as is typical of any VisaNet service offered to Issuers. VisaGold must incorporate as much automated or systematic controls as possible so that management of this service is efficient for Visa, Issuers, and participating Merchants.

# **3 VisaGold Approach**

## *3.1 VisaGold Business Requirements*

The business requirements that relate to VisaGold processing are below. The VisaGold solution must:

1. Increase market momentum of the 3-D Secure rollout.

© 2003 Visa U.S.A. Inc. This information is Confidential and Proprietary, is distributed only by Visa U.S.A. for the use exclusively in operating this Visa-sponsored program, and shall not be duplicated, published, or disclosed, in whole or in part, without the written permission of Visa U.S.A.

2. Require no changes to the 3-D Secure protocol.
3. No/minimal changes to installed ACS or merchant software.
4. In the future, VisaGold will allow Merchant Plug-In's (MPI) and ACS's to migrate to newer versions of the 3-D Secure protocol independently of each other. VisaGold will provide compatibility between these end points via a standardized certification process similar to the VisaNet Certification Management System (VCMS). The requirements for this certification process are outside the scope of this document.

### 3.2 *VisaGold Service and Technical Requirements*

The service and technical requirements that relate to VisaGold processing are below. The VisaGold solution must:

1. Support 3-D Secure message versions 1.0.1 and later. VisaGold will not support 3-D Secure message versions prior to 1.0.1. VisaGold only supports the Core Protocol requirements.
2. Receive and route VEReq transactions from the Directory Server (DS) to the appropriate ACS, return the VERes from the ACS to the DS, and log both messages with the ability to associate the VERes with the VEReq.
3. Receive and route PAREq transactions from an MPI to an ACS, return the PAREs from the ACS to the MPI, and log both messages with the ability to associate the PAREs with the PAREq.
4. Systematically associate a VEReq/VERes message pair with the corresponding PAREq/PAREs message pair.
5. Process and log all activity that occurs between the cardholder and an ACS during the authentication process. If an ACS fails to respond to any request from a cardholder within the specified timeout interval, VisaGold must be able to generate a response on behalf of the ACS, including the submission of a PATransReq to the Authentication History Server (AHS) and handling a PATransRes from the AHS.
6. Validate the format and content of the data values in each supported message. Supported messages include, VEReq, VERes, PAREq, PAREs, PATransReq, and PATransRes.
7. Provide an interface to define, configure, and administer the VisaGold operating parameters. These parameters will include at least the following:

© 2003 Visa U.S.A. Inc. This information is Confidential and Proprietary, is distributed only by Visa U.S.A. for the use exclusively in operating this Visa-sponsored program, and shall not be duplicated, published, or disclosed, in whole or in part, without the written permission of Visa U.S.A.



- VERes timeout value
  - VERes timeout response
  - PAREs timeout value
  - PAREs timeout response
  - Authentication page timeout value
  - Authentication page timeout response
  - Client certificate configuration
  - Primary and Second AHS URL
  - Number of times to attempt connecting to the AHS during PATransReq processing
  - PATransRes timeout value
  - PATransReq retry count
6. Support any HTML 3+ capable Internet client without requiring the use of JavaScript, cookies, or limitation of any kind on the client's chosen hardware or operating system, regardless of version, or other service limiting features.
7. Support 500 page views per second and 100 3-D Secure messages per second per machine. The average time for processing any one page view must not exceed 0.5 seconds. The average time required to process any one 3-D Secure message must not exceed 0.5 seconds, excluding the time associated with the DS, ACS, or other 3-D Secure component's processing time.
- Note: Performance measurements will be calculated using a series of pages with the least possible content (no graphics/images, links, external references, etc.) and only sufficient text to allow the page to proceed to the next processing step. The service operator will calibrate performance of the production service, with live pages, through a separate exercise.
8. Meet 99.9% availability, 24x7x365 with no downtime during VisaGold service updates.
9. Not require the sharing of data or system components across multiple VisaGold servers, i.e., any one individual VisaGold component must not be reliant on any other VisaGold service component in order to complete the

© 2003 Visa U.S.A. Inc. This information is Confidential and Proprietary, is distributed only by Visa U.S.A. for the use exclusively in operating this Visa-sponsored program, and shall not be duplicated, published, or disclosed, in whole or in part, without the written permission of Visa U.S.A.

functions described in this document. The requirement excludes the networking infrastructure required to support communication to the VisaGold service components. Failure of any one service component must not impact the availability of any other service component.

Note: No other option, regardless of capability, is acceptable.

10. All logging must conform to the NCSA extended/combined log format. All logs must be rolled – renamed with a date and timestamp – once per day and at end of each day. Analysis of VisaGold logs will occur on a separate reporting platform (See *VisaGold Reporting Requirements* section).
11. Conform and comply with Visa's Cardholder Information Security Program (CISP) requirements.
12. Use a web server platform which supports the following service support areas:
  - a. Authentication, Authorization, and Access Control
  - b. CGI: Dynamic Content with CGI
  - c. Configuration Files
  - d. Content negotiation
  - e. Environment Variables
  - f. General Performance
  - g. Handlers
  - h. Log Files
  - i. Security
  - j. Server Side Includes
  - k. Server-Wide Configuration
  - l. URL Mapping
  - m. URL Rewriting
  - n. Virtual Hosts

### 3.3 VisaGold Process Flow

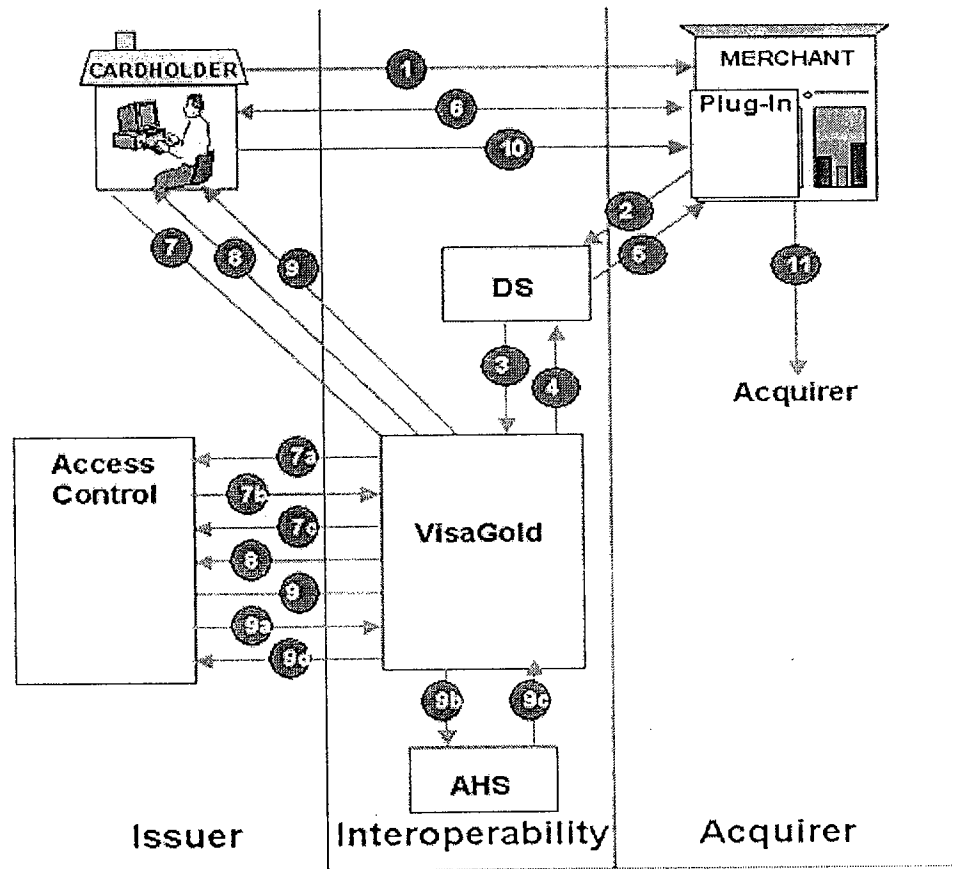
This section describes the Activation Anytime process flow. Refinements may be needed as the business requirements and service rules are evaluated.

The VisaGold process flow approach introduces the concept of a centralized switching device to support the processing of 3-D Secure messages and routing of a cardholder to ACS. VisaGold provides Visa with the ability to:

1. Monitor, record, and report on the VEReq/VERes and PAReq/PARes message flows.

2. Provide a response on behalf of an ACS if the ACS is not available or does not respond in a timely manner.
3. Increase the number and percentage of fully authenticated purchases and reduce breakage associated with cardholder abandonment during the check out process at 3-D Secure-enabled merchant sites.

The steps below described the transaction flow for VisaGold in the 3-D Secure model:



Steps	Description of Steps in the VisaGold Flow
Step 1	Shopper browses at merchant site, adds items to shopping cart, and then finalizes purchase. (Note: Merchant now has all necessary data, including PAN.)
Step 2	Merchant Server Plug-in (MPI) sends PAN to the Visa Directory.

© 2003 Visa U.S.A. Inc. This information is Confidential and Proprietary, is distributed only by Visa U.S.A. for the use exclusively in operating this Visa-sponsored program, and shall not be duplicated, published, or disclosed, in whole or in part, without the written permission of Visa U.S.A.

### 3-D Secure Business Requirements and Technical Approach

VisaGold

May 2003

Step 3	If PAN is in participating card range, Visa Directory queries VisaGold to determine whether authentication is available for the PAN.
Step 4	VisaGold responds to Visa Directory with an enrolled response.  Note: VisaGold does not forward the VEReq message to the ACS at this point. VisaGold generates and returns an acctID, url, and enrolled status of "Y" for all Visa cards.
Step 5	Visa Directory forwards VisaGold response to MPI.
Step 6	MPI sends Payer Authentication Request to VisaGold via shopper's device.
Step 7a	VisaGold receives Payer Authentication Request. VisaGold queries appropriate Access Control Server (ACS) to determine whether authentication is available for the PAN.
Step 7b	ACS responds to VisaGold with an enrolled response.
Step 7c	If the cardholder is enrolled, VisaGold relays the Payer Authentication Request message to the ACS. If the cardholder is not enrolled, VisaGold returns an attempted or unable authenticate response to the MPI (see Step 9, 9c, and 9d).
Step 8	VisaGold relays all interactions between the shopper and ACS.  ACS authenticates shopper using processes applicable to PAN (Password, Chip, PIN, etc.).  ACS formats Payer Authentication Response message with appropriate values and signs it.
Step 9	ACS returns Payer Authentication Response to MPI via shopper's device. ACS sends selected data to Authentication History.
Step 9a	ACS sends the Payer Authentication Transaction Receipt to VisaGold.
Step 9b	VisaGold send the Payer Authentication Transaction Receipt to the Authentication History Server (AHS).
Step 9c	The AHS sends the Payer Authentication Transaction Receipt response to VisaGold.  Note: If VisaGold generates the Payer Authentication Response, VisaGold sends the Payer Authentication Transaction Receipt to AHS.
Step 9d	VisaGold returns the Payer Authentication Transaction Receipt response to ACS.

© 2003 Visa U.S.A. Inc. This information is Confidential and Proprietary, is distributed only by Visa U.S.A. for the use exclusively in operating this Visa-sponsored program, and shall not be duplicated, published, or disclosed, in whole or in part, without the written permission of Visa U.S.A.

3-D Secure Business Requirements and Technical Approach  
VisaGold  
May 2003

---

Step 10	MPI receives Payer Authentication Response and validates Payer Authentication Response signature.
Step 11	Merchant proceeds with authorization exchange with its Acquirer.

### 3.4 VisaGold Reporting Requirements

This section describes the VisaGold reporting requirements. Refinements may be needed as the business requirements and service rules are evaluated. The VisaGold reporting solution must provide reporting in the aggregate and by date, including day of week, and hour for the requirements listed below. The reporting tool must provide the ability to generate ad hoc user defined queries.

1. Total number of page hits, including page hits by page, and errors
2. Aggregate information and information sorted by referring Internet site, or BIN, or 3-D Secure message version:
  - a. Number of VEReq messages received
  - b. Number of VERes's returned, sorted by:
    - i. "Timed out waiting on response from ACS"
    - ii. "Error connecting to ACS (non-timeout condition)"
    - iii. "N" – no enrollment option available
    - iv. "U" – not eligible to enroll
    - v. "Y" – enrolled
    - vi. "Other error/response received (not defined above)"
    - vii. Minimum, maximum, and average response time for VEReq/VERes processing in total and by ACS
  - c. Number of PAREq's received
  - d. Number of authentication pages received, sorted by:
    - i. "Timed out waiting on response from ACS"
    - ii. "Error connecting to ACS (non-timeout condition)"
    - iii. "Other error/response received (not defined above)"

```
<Extension id="visa.3ds.activation_anytime" critical="false">
  <passwordreset>fully qualified URL</passwordreset>
  <issueremail>Issuer VbV Email Address</issueremail >
  <issuerphone>Issuer Customer Service Phone Number</issuerphone>
  <issuerprograminfo>fully qualified URL</issuerprograminfo>
  <issuereenrollment> fully qualified URL</issuereenrollment>
</Extension>
```

## 4 Related Documents

This section describes related documents that contain additional requirements and/or clarification of processing requirements for the VisaGold service.

1. Cardholder Information Security Program, Version 5.5
2. 2. 3-D Secure™ Protocol Specification, Core Functions, 70000-01 v 1.0.2, Updated 9/16/02  
The one on the paytech site is Updated 7/16/02 with Errata as of 01/16/03.  
See <http://international.visa.com/fb/paytech/secure/main.jsp>.